



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/687,694	10/20/2003	Matthew Murray Williamson	1509-458	2845

7590	03/08/2007
HEWLETT-PACKARD COMPANY	
Intellectual Property Administration	
P.O. Box 272400	
Fort Collins, CO 80527-2400	

EXAMINER	
MORAN, RANDAL D	

ART UNIT	PAPER NUMBER
2135	

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
3 MONTHS	03/08/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

Office Action Summary

Application No.

10/687,694

Applicant(s)

WILLIAMSON ET AL.

Examiner

Randal D. Moran

Art Unit

2135

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 20 October 2003.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-41 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-41 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 20 October 2003 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
- Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
- Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☒ All b) ☐ Some * c) ☐ None of:
1. ☒ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☒ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date 5/27/2004 and 10/18/2005
- 4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____
- 5) ☐ Notice of Informal Patent Application
- 6) ☐ Other: _____

DETAILED ACTION

1. Claims 1-44 are pending in this application.
2. The Information Disclosure Statements filed on 5/27/2004 and 10/18/2005 have been considered by the examiner.
3. The preliminary amendment filed on 10/20/2003 has been considered by the examiner.

Claim Objections

4. The following claims are objected to for lack of antecedent basis.
 - **Claim 16-** line 3 recites the limitation "the predetermined size."
 - **Claim 28-** line 2 recites the limitation "said time intervals."

Claim Rejections - 35 USC § 103

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

6. **Claims 1-6, 8, 9, 14-18, 20, 21, 23, 29-34, and 41** are rejected under 35 U.S.C. 103(a) as being unpatentable over **Alexander Shipp (GB 2 367 714)**, hereafter "Shipp," **in view of Andersen (US 6,122,740)**, hereafter "Andersen."

7. Alexander Shipp (GB 2 367 714) was submitted in the IDS filed on 5/27/2004.

8. Considering **Claim 1**, Shipp discloses a method of monitoring propagation of viruses within a network of hosts (abstract- lines 1-3), comprising the steps of: storing in a buffer data relating to requests which identify a destination host not in the record (p. 12- lines 3-5, once the criterion for an infected message has been found, i.e. a host not in the record, holding the request in a temporary storage).

Shipp does not explicitly disclose establishing a record which is at least indicative of identities of hosts within the network to whom data has been sent by a first host ("destination hosts"); during a first time interval 1) comparing (a) identities of destination hosts identified in requests to send data from the first host and (b) identities of destination hosts identified in the record; transmitting all requests to send data.

Andersen does explicitly disclose establishing a record which is at least indicative of identities of hosts within the network to whom data has been sent by a first

host ("destination hosts") (Fig. 3, Fig 5- item 512, column 5- lines 19-23, column 6- lines 56-59); during a first time interval (column 8- lines 64-68, column 9- line 1) comparing (a) identities of destination hosts identified in requests to send data from the first host and (b) identities of destination hosts identified in the record (column 6- lines 56-59); transmitting all requests to send data (column 5- lines 51-54).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the teachings of Shipp by keeping a log of network requests and comparing new requests to the log before transmitting all requests as taught by Andersen in order to identify patterns characteristic of a virus outbreak and take corrective action (Shipp- abstract).

9. Considering **Claims 29 and 41**, Andersen discloses a method of operating a first host within a network of a plurality of hosts comprising the steps of (Fig. 1): over the course of a first time interval (column 8- lines 64-68, column 9- line 1), monitoring creation of sockets within the first host to identify destination hosts identified therein (column 4- lines 53-67, column 5- lines 1-8); comparing identities of destination hosts monitored during the first time interval with destination host identities in a record (column 6- lines 56-59);

Andersen does not explicitly disclose storing data from all sockets which identify destination hosts not in the record.

Shipp does explicitly disclose storing data from all sockets which identify destination hosts not in the record (p. 12- lines 3-5, once the criterion for an infected message has been found, i.e. a host not in the record, holding the request in a temporary storage).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the teachings of Andersen by storing data from all sockets which identify data not in the record as taught by Shipp in order to identify patterns characteristic of a virus outbreak and take corrective action).

10. Considering **Claim 2 and 32**, the combination of Andersen and Shipp discloses the record is established by monitoring identities of destination hosts to whom requests have been transmitted during a second time interval, which precedes the first time interval (Andersen- column 6- lines 3-13).
11. Considering **Claims 3 and 31**, the combination of Andersen and Shipp discloses the record contains a predetermined maximum number of destination host

identities, the maximum number being defined in accordance with a policy (Shipp- p. 11- lines 22-24 and 29, p.13- line 15 and 36-37).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Andersen and Shipp for the benefit of creating a maximum threshold that once exceeded, will result in the flagging of a potential virus (Shipp- p. 13- lines 36-37).

12. Considering **Claim 4 and 33**, the combination of Andersen and Shipp discloses the policy additionally defines a maximum number of destination host identities not in the record, to whom requests may be legitimately transmitted in accordance with policy (Shipp- p.11- lines 22-29, Andersen- column 5- lines 51-54).
13. Considering **Claim 5 and 34**, the combination of Andersen and Shipp discloses the step, at the end of any given time interval, of deleting from the buffer data relating to requests transmitted during the given time interval in accordance with policy (Shipp- p.12- lines 3-5).
14. Considering **Claim 6**, the combination of Andersen and Shipp discloses the step, at the end of the given time interval, of updating the record to reflect identities of

hosts identified in requests which are transmitted in accordance with policy during the given time interval (Andersen- column 8- lines 56-68, column 9- line 1).

15. Considering **Claim 8**, the combination of Andersen and Shipp discloses the stored data is offered in a buffer and includes a copy of a socket created to send data in accordance with a request (Andersen- column 4- lines 63-68, column 5- lines 1-8).
16. Considering **Claims 9 and 30**, the combination of Andersen and Shipp discloses the socket enables identification of at least one application program at whose behest the socket is created (Andersen- column 5- lines 27-34).
17. Considering **Claims 14 and 28**, the combination of Andersen and Shipp discloses said time periods are of equal duration to at least one of said time intervals (Shipp- p. 11- line 26, p. 13- line 1).
18. Considering **Claim 15**, the combination of Andersen and Shipp discloses the step of monitoring the rate of increase in the size of the buffer, and in the event that the rate of increase in the size of the buffer exceeds a predetermined rate, generating a warning (Shipp- p. 13).

19. Considering **Claim 16**, the combination of Andersen and Shipp discloses monitoring the increase in the size of the buffer per time interval, and in the event that the increase in the size of the buffer in any given time interval exceeds the predetermined size, generating a warning (Shipp- p. 11- lines 22-39, p. 13).
20. Considering **Claim 17**, the combination of Andersen and Shipp discloses the step of monitoring the size of the buffer, and in the event that the buffer exceeds a predetermined size for a predetermined number of successive time intervals, generating a warning (Shipp- p. 11- lines 22-39, p. 13).
21. Considering **Claim 18**, the combination of Andersen and Shipp discloses at least one parameter selected from the group consisting of: number of destination hosts in the record; threshold number of requests identifying destination hosts not in the record and defining a state of viral infection, is varied with time (Shipp- p. 11- lines 22-39, p. 13).
22. Considering **Claim 20**, the combination of Andersen and Shipp discloses at least one of the parameters is varied in response to a perceived threat level (Shipp- p. 11- lines 22-39, p. 13).

23. Considering **Claim 21**, the combination of Andersen and Shipp discloses at least one of the parameters is changed between a first set of values and a second set of values at a predetermined rate (Shipp- p. 11- lines 22-39, p. 13).
24. Considering **Claim 23**, the combination of Andersen and Shipp discloses at least one parameter selected from the group consisting of: number of destination hosts in the record; threshold number of requests identifying destination hosts not in the record and defining a state of viral infection, is determined by performing an automated search on a set of data indicative of normal network traffic (Shipp- p. 11- lines 22-39, p. 13).
25. Considering **Claims 35 and 38**, the combination of Andersen and Shipp discloses the step, in the event that the number of socket data items stored exceeds a predetermined value, of storing outgoing packets from the first host (Andersen- column 4- lines 64-67, column 5- lines 1-8, Shipp- p.12- 2-5, p.13).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the combination of Andersen and Shipp by using the socket data from Andersen as a parameter for Shipp to determine if the threshold has been reached. This would provide the benefit of not only being able to track emails, but allowing the monitoring of the port data itself.

26. **Claims 7** is rejected under 35 U.S.C. 103(a) as being unpatentable over **Shipp and Andersen** in view of **Maher, III et al. (US 7,058,974)**, hereafter "Maher."
27. Considering **Claim 7**, the combination of Andersen and Shipp does not explicitly disclose the step of updating the record to reflect the identity of the predetermined maximum number of destination host identities to whom data has most recently been sent in accordance with policy.

Maher does explicitly disclose the step of updating the record to reflect the identity of the predetermined maximum number of destination host identities to whom data has most recently been sent in accordance with policy (column 7- lines 16-26, the state awareness of the traffic flow is taken to be the most recently sent hosts).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the teachings of Andersen and Shipp by updating the record to include the most recent destination hosts as taught by Maher for the benefit of keeping an up to date list of recent session ids to ensure that the proper linked list information is retrieved (Maher- lines 41-51).

28. **Claims 10-13** are rejected under 35 U.S.C. 103(a) as being

unpatentable over **Shipp and Andersen** in view of **Ramanujan (US 5,341,491)**, hereafter "Ramanujan."

29. Considering **Claims 10 and 12**, the combination of Andersen and Shipp discloses allowing the un-impeded passage of data from the first host to other hosts not in the record (column 5, lines 51-54).

The combination of Andersen and Shipp does not disclose determining the value of parameter ("slack") based upon a number of successive time periods that pass when no new requests are made to send data from the first host to hosts not in the record; and slack exceeds a predetermined value.

Ramanujan does disclose determining the value of parameter ("slack") based upon a number of successive time periods that pass when no new requests are made to send data from the first host to hosts not in the record (column 2- lines 37-44, the refusal counter holds the variable of mslack); and slack exceeds a predetermined value (column 2- lines 44-48).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the teachings of Andersen and Shipp by determining a variable based upon the number of successive attempts that are made to perform an action as taught by Ramanujan for the benefit of being

able to generate a response to a predetermined condition such as locking resources of a computer or allowing further network access. Ramanujan discloses incrementing a counter for successive refused attempts to access a network resource. Once the counter reaches a predetermined value, the resource is locked. It would have been obvious to use the same counter in the combination of Andersen and Shipp to determine when to allow the unimpeded access to the network.

30. Considering **Claim 11**, the combination of Andersen, Shipp, and Ramanujan discloses slack is determined based upon the number of successive time periods for which the buffer is empty (Ramanujan- column 10- lines 10-24).
31. Considering **Claim 13**, the combination of Andersen, Shipp, and Ramanujan discloses the value of slack is decremented each time an un-impeded passage of data from the first host to a host not in the record is allowed (Ramanujan – column 10- lines 39-50, as the lock queue goes from empty to inhabited the counter is incremented and decremented to determine whether to lock the resource. In the combination, this would cause the variable to be decremented each time data not in the record is allowed passage.)

Art Unit: 2135

32. Considering **Claim 24-27**, are rejected for the same reasons as Claim 10-13 above. It would have been obvious to one of ordinary skill in the art at the time of the invention to perform the same tasks using a multiple recipient email.
33. **Claims 19-22** are rejected under 35 U.S.C. 103(a) as being unpatentable over **Shipp and Andersen** in view of **Cunningham et al. (EP 0 986 229)**.
34. Cunningham et al. (EP 0 986 229) was submitted in the IDS filed on 5/27/2004.
35. Considering **Claims 19 and 22**, the combination of Andersen and Shipp does not explicitly disclose at least one parameter is varied as a function of the time of day.

Cunningham does explicitly disclose at least one parameter is varied as a function of the time of day (column 5- lines 33-37).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the teachings of Andersen and Shipp by having a parameter that is varied as a function of time as taught by Cunningham for the benefit of using parameters in the rule base that are familiar to the users (Cunningham- column 5- lines 33-37).

Art Unit: 2135

36. **Claims 36, 37, 39, and 42** are rejected under 35 U.S.C. 103(a) as being unpatentable over **Shipp and Andersen** in view of **Anderson (US 2002/0013858)**, hereafter "858."

37. Considering **Claim 36 and 39**, the combination of Andersen and Shipp does not explicitly disclose packets having a designated destination IP address are stored.

858 does explicitly disclose packets having a designated destination IP address are stored ([0046]).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the teachings of Andersen and Shipp by storing designated IP addresses for the benefit of being able to isolate certain addresses for future use.

38. Considering **Claim 37 and 42**, the combination of Andersen and Shipp does not explicitly disclose the step of establishing the predetermined IP address from the stored socket data.

It would have been obvious to one of ordinary skill in the art at the time of the invention to use the socket data to determine the IP address to be stored.

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the teachings of Andersen and Shipp to establish the IP address from the stored socket data to use data that is relevant to the network flow to store future packets.

Conclusion

39. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Randal D. Moran whose telephone number is 571-270-1255. The examiner can normally be reached on M-F: 7:00 - 4:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on 571-272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

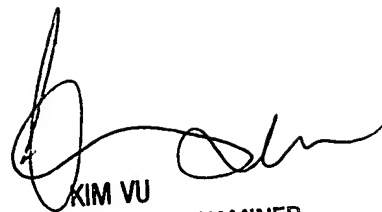
Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Art Unit: 2135

Randal D. Moran

/RDM

2/7/07

A handwritten signature in black ink, appearing to read 'Kim Vu', written over a printed name.

KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100